consideration is required by Applicant's amendment since the amended Claim 18 includes the limitations of Claim 19 now canceled.

Reconsideration is respectfully requested of the rejection of Claims 1, 3-11 and 13-20 under 35 USC 103(a) as being unpatentable over TOMKO (US 5,712,912) in view of CHAUM (US 4,529,870).

The invention relates to a security token comprising a biometric sensor that provides a first biometric key of a current user of the security token based upon a biometric measure of the current user. The security token also comprises a storage element that stores an encryption of a security key, the encryption being based on a second biometric key of an authorized user. The security token further comprises a biometric decrypter, operably coupled to the biometric sensor and the storage element, that decrypts the encryption of the security key, producing thereby a decrypted security key that is equal to the security key when the first biometric key is equivalent to the second biometric key. The security token comprises an authentication encrypter, operably coupled to the biometric decrypter, that encrypts a challenge parameter to produce a response parameter that is based upon the decrypted security key.

Tomko

Tomko discloses a PIN generating apparatus comprising a PIN encrypting device (Fig.1A) and a PIN decrypting device (Fig.1B). The PIN encrypting device comprises a random character generator that generates a digital PIN. The Pin is then encrypted with the

fingerprint-related information provided by the user and the encrypted PIN is then stored in storage means.

The decrypting device is used to obtain access to a communication network, financial device or to another system, where a PIN is required. The individual places his finger and a processor 204 uses the fingerprint-related information generated from the finger as a key to decrypt the encrypted PIN. If the fingerprint is the same as the one used during encryption, the processor decrypts the PIN and sends it to the device or system requesting the PIN (col.3, l.42-col.4, l.28).

Chaum

Chaum discloses an external system 101 and cryptographic device 103 of a card 108. The external system 101 provides the cryptographic device 103 its system ID and challenge data which it has generated for use with a particular identification transaction. The owner of the card 108 provides the cryptographic device 103 a secret owner ID. The owner ID is used by the encryption/decryption circuitry of the device 103 to decrypt the system key associated with the external system 101 maintained in secure memories of the device 103. The external system data stored in the cryptographic device 103 is preferably maintained in an encrypted form so that unless the owner ID is available to the cryptographic device 103, a third party may not access or recover the encrypted data (col.12, l.9-col.13, l.-7).

The cryptographic device 103 generates a random value and encrypts this random value using an external system key stored in the cryptographic device 103 and also known to the system 101 (col.13, l.8-13).

The external system 101 and the device 103 then generate a new temporary cryptographic key unique to this identification

process. The key is generated by a previously agreed upon algorithm from data known to both the external system 101 and the cryptographic device 103. This data may include the challenge, the system key and/or the random value (col.14, l.34-50)

After operation of the temporary cryptographic key by both the external system 101 and cryptographic device 10, they each enter into a "secured communications mode" and further communication between the external system 101 and device 103 are encrypted utilizing the temporary key.

Tomko clearly differentiates from the invention in the sense that Tomko does not disclose the apparatus comprising an authentication encrypter that encrypts a challenge parameter using the decrypted PIN provided by the processor 204 of the decrypting device of Fig.2B.

Chaum discloses generating the temporary cryptographic key using the challenge data provided by the external device to the cryptographic device. However Chaum does not disclose encrypting the challenge data to produce a response parameter. The temporary cryptographic key of Chaum differs from the response parameter of the invention in the sense that Chaum discloses a key to be used in encryption and the invention discloses an encrypted response parameter.

In addition, Chaum neither suggests nor discloses producing from a challenge data, an encrypted response parameter that is based upon the decrypted security key. In Chaum, the system external data decrypted using the owner ID is not used as a basis to encrypt the challenge data provided by the external system

Chaum neither mentions nor discloses the secret owner ID being a biometric key of the user.

Neither Tomko nor Chaum suggests or teaches the claim limitation of an authentication encrypter that encrypts a challenge parameter to produce a reponse parameter that is based upon the decrypted security key. So even if the teachings of both documents were to be combined, the result would still not be a security token of the invention as claimed in Claim 1 or a security system of Claim 9. The Examiner has thus not met the burden of showing a prima facie case of obviousness and the rejection of the claims under 35 USC 103(a) is incorrect.

It is respectfully submitted that independent Claim 1, 9 and 18 are patentable over Tomko in view of Chaum. It is also respectfully submitted that dependent Claims 3-8, 10-11, 13-17 and 20 are patentable over Tomko in view of Chaum at least based on their dependencies.

Applicant respectfully submits that he has answered all issues raised by the Examiner and that the application is accordingly in condition for allowance. Such allowance is therefore respectfully requested.

Please charge any fees other than the issue fee to deposit account 14-1270.

Please credit any overpayments to the same account.

Respectfully submitted,

Dated: April 10, 2002

By _____
Gwenaelle Le Pennec
Limited Recognition under 37 C.F.R 10.9(b)
(408) 617-4837